UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/047,564	01/14/2002	Nobuyuki Koike	3169.66103	4686

7590 09/08/2005

Patrick G. Burns, Esq.
GREER, BURNS & CRAIN, LTD.
Suite 2500
300 South Wacker Dr.
Chicago, IL 60606

EXAMINER	
AU, SCOTT D	

ART UNIT	PAPER NUMBER
2635	

DATE MAILED: 09/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/047,564	KOIKE, NOBUYUKI	
	Examiner	Art Unit	
	Scott Au	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4,14,16-18,28,30-32 and 42-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-4,14,16-18,28,30-32 and 42-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to applicant's response to the RCE, which is filed July 14, 2005.

The application of Koike for a "Key information issuing device" filed August 31, 2001 has been examined.

Claims 2,3,4,14,16,17,18,28,30,31,32 and 42-48 are pending.

Claims 1,5-13,15,19-27,29, and 33-41 are cancelled.

Response to Arguments

Applicant's amendments and argument to the rejected claims are insufficient to distinguish the claimed invention from the cited prior arts to overcome the rejection of said claims under 35 U.S.C 103(a) as discussed below. Applicant's amendment and argument with respected to the pending claims 1-8 and 13, filed on November 11, 2003, have been fully considered but they are not persuasive for at least the following reasons.

On page 14, paragraph 3, Applicant's arguments with respect to the invention Bonder et al. in view of Cregger et al. and Desai that one ordinary skill in the art would not have been motivated to combine the references.

In response to Applicant's argument that there is no suggestion to combine the references, the Examiner recognizes that references cannot be arbitrarily combined and

that there must be some reason why one skilled in the art would be motivated to make the proposed combination of primary and secondary references. *In re Nomiya*, 184 USPQ 607 (CCPA 1975). However, there is no requirement that a motivation to make the modification be expressly articulated. The test for combining references is what the combination of disclosures taken as whole would suggest to one of ordinary skill in the art. *In re McLaughlin*, 170 USPQ 209 (CCPA 1971).

Bonder et al. suggest the security system can control and grant access to a secure area, or to a secure database. A separate key programming system is located at a central programming location, and is used to initialize and change data stored in the memory. The separate programming system includes a microcontroller, a random access memory, a keyboard for input of alphanumeric data, a fingerprint scanner, a key receptacle for inserting an intelligent key to program, a power/data interface to interface with the key, and a temporary memory which stores user data during programming but is erased after programming of the intelligent key (col. 3 lines 10-22).

In the same field endeavor of security system, Cregger et al. suggest a programmer device (301a) includes a pair of look-up tables (902 and 903) containing a listing of various identification numbers and encryption key codes for each lock of the system (col. 5 lines 55-65).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to use table storage of Cregger et al. in the

programming device of Bonder et al. with the motivation for doing so would allow the programming device to have record of the key code in case the key is lost or stolen.

In the same field of endeavor of security system, Desai discloses the wireless vehicle control teaches code to the key/fob combination. A series of steps to move the key/fob combination into a learn mode is utilized, and then the code is then taught from the vehicle scanning receiver to the key/fob combination.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to (37) (i.e. key/fob combination) is a wireless operation device wirelessly connected to device (22) (i.e. control located in the vehicle) and includes a input module (48) (i.e. key pad) inputting the key information in contact with said device (22) (i.e. control located in the vehicle), and said output module includes (i.e. transmitter of the control 22) a contact module outputting the key information in contact with said key information input module of Desai in the information issuing device of Bonder et al. in view of Cregger et al. with the motivation for doing so would allow the retaining device to communicate wirelessly with the issuing device as an alternative way of communicating through physical contact.

Notice of Non-Compliant Amendment (37 CFR 1.121)

According to claims 47-48, the claims should have been provided with the proper status identifier. The claims should be identified as (New) instead of (Original).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2,3,4,14,16,17,18,28,30,31,32 and 42-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bonder et al. (US# 6,078,265) in view of Cregger et al. (US# 6,384,711), Weiss et al. (US# 6,522,240) and further in view of Desai (US# 6,377,173).

Referring to claim 2, Bonder et al. disclose a key information issuing device (i.e. see Figure 2) issuing key information to a key information retaining device (11) (i.e. intelligent key), comprising:

an authentication module (24) (i.e. scanner) authenticating an issuer of the key information;

an output module (26) (i.e. power/data interface) outputting the key information to said key information retaining device (11) (i.e. intelligent key); and

a recording module (22) (i.e. memory),

wherein the key information is issued in response to an indication of the authenticated issuer (col. 4 lines 5-62 and col. 5 lines 20-62; see Figures 1-2 and 4). However,

Bonder et al. did not explicitly disclose a recording module recording a mapping of the issued key information to information of said key information retaining device.

In the same field of endeavor programmable key device, Cregger et al. disclose a recording module (902 and 903) (i.e. storage tables) recording a mapping of the issued key information to information of said key information retaining device (104a) (i.e. key unit) (col. 5 line 38 to col. 6 line 6) in order to identify the key corresponding to that lock.

One ordinary skill in the art understands that storage table of Cregger et al. is desirable in the programming device of Bonder et al. because Bonder et al. suggest random access memory (22) and temporary memory (27) as a storage in the programming device (col. 5 lines 19-32) and Cregger et al. suggest a programmer device (301a) includes a pair of look-up tables (902 and 903) containing a listing of various identification numbers and encryption key codes for each lock of the system (col. 5 lines 55-65). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to use table storage of Cregger et al. in the programming device of Bonder et al. with the motivation for doing so would allow the programming device to have record of the key code in case the key is lost or stolen.

However, Cregger in view of Bonder et al. did not explicitly disclose a receiving module receiving wireless signals from said key information retaining device; and a decoding module decoding the information contained in the wireless signals and encrypted with the key information; wherein said key information retaining device is a

wireless operation device wirelessly connected to an information device and includes a key information input module inputting the key information in contact with said key information issuing device, and said output module includes a contact module outputting the key information in contact with said key information input module.

In the same field of endeavor of information issuing device, Weiss et al. disclose further comprising: a receiving module (11) (i.e. transmitter/receiver) receiving wireless signals from said key information retaining device; and a decoding module (12) (i.e. decoder) decoding the information contained in the wireless signals and (i.e. encoder) encrypted with the key information (col. 2 lines 6-39; see Figure 1).

One of ordinary skill in the art understands that the base station communicate with the control element of Weiss et al. is desirable in the communication between the intelligent key and the programming device of Bonder et al. in view of Cregger et al. because Bonder et al. suggest the security system of the present invention could be utilized in an embodiments to control and grant access to a secure area such as a building, room, vault, cabinet, safety deposit box, etc., or to control and grant access to a secure database or any other secure system wherein control and access concerns secure or secret matters (col. 3 line 63 to col. 4 line 4) and Weiss et al. disclose a base station 10 can, for example, be a part of the access control system of an automobile or of a building, or it can belong to a computer, for example, or another appliance. A device which is here referred to as a control element 20 is functionally assigned to base station 10 and acts on it without physical contact (col. 1 line 63 to col. 2 line 5).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to a receiving module (11) (i.e. transmitter/receiver) receiving wireless signals from said key information retaining device; and a decoding module (12) (i.e. decoder) decoding the information contained in the wireless signals and (i.e. encoder) encrypted with the key information of Weiss et al. in the information issuing device of Weiss et al. in the information issuing device of Bonder et al. in view of Cregger et al. with the motivation for doing so would allow the retaining device to gain access to a secured system.

However, Bonder et al. in view of Cregger et al. and Weiss et al. did not explicitly disclose wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a key information input module inputting the key information in contact with said key information issuing device, and said output module includes a contact module outputting the key information in contact with said key information input module.

In the same field of endeavor of security system, Desai discloses wherein said key information retaining device (37) (i.e. key/fob combination) is a wireless operation device wirelessly connected to an information device (22) (i.e. control located in the vehicle) and includes a key information input module (48) (i.e. key pad) inputting the key information in contact with said key information issuing device (22), and said output module includes (i.e. transmitter of the control 22) a contact module outputting the key information in contact with said key information input module (col. 1 lines 50-57, col. 2

line 45 to col. 12 and col. 3 line 53 to col. 4 line 14; see Abstract and Figure 1) in order train the fob with the desire operation functions.

One of ordinary skill in the art understands that wireless operation system of Desai is desirable in the key programming device of Bonder et al. in view of Cregger et al. and Weiss et al. because Bonder et al. suggest that in an alternative embodiments, the motor vehicle could be any type of motor vehicle such as truck, bus, motorcycle, boat, snowmobiles, etc. Moreover, the security system could be utilized to control and grant access to a secure area such as a building, room, vault, cabinet or grant access to a secure database or any type of secure system (col. 3 line 63 to col. 4 lines 5) and Desai discloses the vehicle control teaches code to the key/fob combination. A series of steps to move the key/fob combination into a learn mode is utilized, and then the code is then taught from the vehicle scanning receiver to the key/fob combination.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include key information retaining device (37) (i.e. key/fob combination) is a wireless operation device wirelessly connected to an information device (22) (i.e. control located in the vehicle) and includes a key information input module (48) (i.e. key pad) inputting the key information in contact with said key information issuing device (22), and said output module includes (i.e. transmitter of the control 22) a contact module outputting the key information in contact with said key information input module of Desai in the information issuing device of Bonder et al. in view of Cregger et al. and Weiss et al. with the motivation for doing so

would allow the retaining device to communicate wirelessly with the issuing device as an alternative way of communicating through physical contact.

Referring to claim 3, Bonder et al. in view of Cregger et al., Weiss et al. and Desai disclose the key information issuing device issuing key information to a key information retaining device, to the extent as claimed with respect to claim 1 above, Desai discloses the device further comprising: wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a medium input module (48) (i.e. key pad) inputting information from a recording medium, and said output module (i.e. transmitter of the vehicle control) includes a recording medium write module writing the information to said recording medium, and issues the key information through said recording medium (col. 1 lines 48-57, col. 2 line 45 to col. 12 and col. 3 line 53 to col. 4 line 14; see Abstract and Figure 1). It is inherent for the key/fob and vehicle control with recording medium within in order to store the codes.

Referring to claim 4, Bonder et al. in view of Cregger et al., Weiss et al. and Desai disclose the key information issuing device issuing key information to a key information retaining device, to the extent as claimed with respect to claim1 above, Weiss et al. disclose the device further comprising: wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a near communication module incapable of performing

communications beyond a predetermined distance, and said output module includes a near communication module incapable of performing the communications with said key information retaining device beyond a predetermined distance, and issues the key information through said near communication module (col. 3 lines 21-28 and col. 4 lines 1-10). (i.e. The near communication module of retaining device is incapable of communicating with the output module of the issuing device when is out-of-ranged).

Referring to claim 16, Bonder et al. disclose a key information managing method of managing key information issued to a key information retaining device (11) (i.e. intelligent key), comprising: (24) (i.e. scanner) authenticating an issuer of the key information; (21) (i.e. microcontroller) generating key information; (26) (i.e. power/data interface) outputting the key information to said key information retaining device (11) (i.e. intelligent key) (col. 4 lines 5-62 and col. 5 lines 20-62; see Figures 1-2 and 4).

However, Bonder et al. did not explicitly recording a mapping of the issued key information to information of said key information retaining device.

In the same field of endeavor programmable key device, Cregger et al. disclose a recording module (902 and 903) (i.e. storage tables) recording a mapping of the issued key information to information of said key information retaining device (104a) (i.e. key unit) (col. 5 line 38 to col. 6 line 6) in order to identify the key corresponding to that lock.

One ordinary skill in the art understands that storage table of Cregger et al. is desirable in the programming device of Bonder et al. because Bonder et al. suggest

random access memory (22) and temporary memory (27) as a storage in the programming device (col. 5 lines 19-32) and Cregger et al. suggest a programmer device (301a) includes a pair of look-up tables (902 and 903) containing a listing of various identification numbers and encryption key codes for each lock of the system (col. 5 lines 55-65).Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to use table storage of Cregger et al. in the programming device of Bonder et al. with the motivation for doing so would allow the programming device to have record of the key code in case the key is lost or stolen.

However, Cregger in view of Bonder et al. did not explicitly disclose a receiving module receiving wireless signals from said key information retaining device; and a decoding module decoding the information contained in the wireless signals and encrypted with the key information; wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a key information input module inputting the key information in contact with said key information issuing device, and wherein output module includes a contact module outputting the key information in contact with said key information input module.

In the same field of endeavor of information issuing device, Weiss et al. disclose further comprising: a receiving module (11) (i.e. transmitter/receiver) receiving wireless signals from said key information retaining device; and a decoding module (12) (i.e. decoder) decoding the information contained in the wireless signals and (i.e. encoder) encrypted with the key information (col. 2 lines 6-39; see Figure 1).

One of ordinary skill in the art understands that the base station communicate with the control element of Weiss et al. is desirable in the communication between the intelligent key and the programming device of Bonder et al. in view of Cregger et al. because Bonder et al. suggest the security system of the present invention could be utilized in an embodiments to control and grant access to a secure area such as a building, room, vault, cabinet, safety deposit box, etc., or to control and grant access to a secure database or any other secure system wherein control and access concerns secure or secret matters (col. 3 line 63 to col. 4 line 4) and Weiss et al. disclose a base station 10 can, for example, be a part of the access control system of an automobile or of a building, or it can belong to a computer, for example, or another appliance. A device which is here referred to as a control element 20 is functionally assigned to base station 10 and acts on it without physical contact (col. 1 line 63 to col. 2 line 5). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to a receiving module (11) (i.e. transmitter/receiver) receiving wireless signals from said key information retaining device; and a decoding module (12) (i.e. decoder) decoding the information contained in the wireless signals and (i.e. encoder) encrypted with the key information of Weiss et al. in the information issuing device of Weiss et al. in the information issuing device of Bonder et al. in view of Cregger et al. with the motivation for doing so would allow the retaining device to gain access to a secured system.

However, Bonder et al. in view of Cregger et al. and Weiss et al. did not explicitly disclose wherein said key information retaining device is a wireless operation device

wirelessly connected to an information device and includes a key information input module inputting the key information in contact with said key information issuing device, and said output module includes a contact module outputting the key information in contact with said key information input module.

In the same field of endeavor of security system, Desai discloses wherein said key information retaining device (37) (i.e. key/fob combination) is a wireless operation device wirelessly connected to an information device (22) (i.e. control located in the vehicle) and includes a key information input module (48) (i.e. key pad) inputting the key information in contact with said key information issuing device (22), and said output module includes (i.e. transmitter of the control 22) a contact module outputting the key information in contact with said key information input module (col. 1 lines 50-57, col. 2 line 45 to col. 12 and col. 3 line 53 to col. 4 line 14; see Abstract and Figure 1) in order train the fob with the desire operation functions.

One of ordinary skill in the art understands that wireless operation system of Desai is desirable in the key programming device of Bonder et al. in view of Cregger et al. and Weiss et al. because Bonder et al. suggest that in an alternative embodiments, the motor vehicle could be any type of motor vehicle such as truck, bus, motorcycle, boat, snowmobiles, etc. Moreover, the security system could be utilized to control and grant access to a secure area such as a building, room, vault, cabinet or grant access to a secure database or any type of secure system (col. 3 line 63 to col. 4 lines 5) and Desai discloses the vehicle control teaches code to the key/fob combination. A series

of steps to move the key/fob combination into a learn mode is utilized, and then the code is then taught from the vehicle scanning receiver to the key/fob combination.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include key information retaining device (37) (i.e. key/fob combination) is a wireless operation device wirelessly connected to an information device (22) (i.e. control located in the vehicle) and includes a key information input module (48) (i.e. key pad) inputting the key information in contact with said key information issuing device (22), and said output module includes (i.e. transmitter of the control 22) a contact module outputting the key information in contact with said key information input module of Desai in the information issuing device of Bonder et al. in view of Cregger et al. and Weiss et al. with the motivation for doing so would allow the retaining device to communicate wirelessly with the issuing device as an alternative way of communicating through physical contact.

Referring to claim 17, Bonder et al. in view of Cregger et al., Weiss et al. and Desai disclose the key information managing method of managing key information issued to a key information retaining unit, to the extent as claimed with respect to claim 16 above, Desai discloses further wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a medium input module (48) (i.e. key pad) inputting information from a recording medium, and said output module (i.e. transmitter of the vehicle control) includes a recording medium write module writing the information to said recording medium, and

issues the key information through said recording medium (col. 1 lines 48-57, col. 2 line 45 to col. 12 and col. 3 line 53 to col. 4 line 14; see Abstract and Figure 1). It is inherent for the key/fob and vehicle control with recording medium within in order to store the codes.

Referring to claim 18, Bonder et al. in view of Cregger et al., Weiss et al. and Desai disclose the key information managing method of managing key information issued to a key information retaining unit, to the extent as claimed with respect to claim 16 above, Weiss et al. disclose wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a near communication module incapable of performing communications beyond a predetermined distance, and wherein issues the key information through said near communication module (col. 3 lines 21-28 and col. 4 lines 1-10). (i.e. The near communication module of retaining device is incapable of communicating with the output module of the issuing device when is out-of-ranged).

Referring to claim 30, Bonder et al. disclose a readable-by-computer recording medium recorded with a program executed by a computer to manage key information issued to a key information retaining device (11) (i.e. intelligent key), comprising: (24) (i.e. scanner) authenticating an issuer of the key information; (21) (i.e. microcontroller) generating key information; (26) (i.e. power/data interface) outputting the key

information to said key information retaining device (11) (i.e. intelligent key) (i.e. intelligent key) (col. 4 lines 5-62 and col. 5 lines 20-62; see Figures 1-2 and 4).

However, Bonder et al. did not explicitly recording a mapping of the issued key information to information of said key information retaining device.

In the same field of endeavor programmable key device, Cregger et al. disclose a recording module (902 and 903) (i.e. storage tables) recording a mapping of the issued key information to information of said key information retaining device (104a) (i.e. key unit) (col. 5 line 38 to col. 6 line 6) in order to identify the key corresponding to that lock.

However, Cregger in view of Bonder et al. did not explicitly disclose a receiving module receiving wireless signals from said key information retaining device; and a decoding module decoding the information contained in the wireless signals and encrypted with the key information; wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a key information input module inputting the key information in contact with said key information issuing device, and wherein output module includes a contact module outputting the key information in contact with said key information input module.

In the same field of endeavor of information issuing device, Weiss et al. disclose further comprising: a receiving module (11) (i.e. transmitter/receiver) receiving wireless signals from said key information retaining device; and a decoding module (12) (i.e. decoder) decoding the information contained in the wireless signals and (i.e. encoder) encrypted with the key information (col. 2 lines 6-39; see Figure 1).

One of ordinary skill in the art understands that the base station communicate with the control element of Weiss et al. is desirable in the communication between the intelligent key and the programming device of Bonder et al. in view of Cregger et al. because Bonder et al. suggest the security system of the present invention could be utilized in an embodiments to control and grant access to a secure area such as a building, room, vault, cabinet, safety deposit box, etc., or to control and grant access to a secure database or any other secure system wherein control and access concerns secure or secret matters (col. 3 line 63 to col. 4 line 4) and Weiss et al. disclose a base station 10 can, for example, be a part of the access control system of an automobile or of a building, or it can belong to a computer, for example, or another appliance. A device which is here referred to as a control element 20 is functionally assigned to base station 10 and acts on it without physical contact (col. 1 line 63 to col. 2 line 5).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to a receiving module (11) (i.e. transmitter/receiver) receiving wireless signals from said key information retaining device; and a decoding module (12) (i.e. decoder) decoding the information contained in the wireless signals and (i.e. encoder) encrypted with the key information of Weiss et al. in the information issuing device of Weiss et al. in the information issuing device of Bonder et al. in view of Cregger et al. with the motivation for doing so would allow the retaining device to gain access to a secured system.

However, Bonder et al. in view of Cregger et al. and Weiss et al. did not explicitly disclose wherein said key information retaining device is a wireless operation device

wirelessly connected to an information device and includes a key information input module inputting the key information in contact with said key information issuing device, and said output module includes a contact module outputting the key information in contact with said key information input module.

In the same field of endeavor of security system, Desai discloses wherein said key information retaining device (37) (i.e. key/fob combination) is a wireless operation device wirelessly connected to an information device (22) (i.e. control located in the vehicle) and includes a key information input module (48) (i.e. key pad) inputting the key information in contact with said key information issuing device (22), and said output module includes (i.e. transmitter of the control 22) a contact module outputting the key information in contact with said key information input module (col. 1 lines 50-57, col. 2 line 45 to col. 12 and col. 3 line 53 to col. 4 line 14; see Abstract and Figure 1) in order train the fob with the desire operation functions.

One of ordinary skill in the art understands that wireless operation system of Desai is desirable in the key programming device of Bonder et al. in view of Cregger et al. and Weiss et al. because Bonder et al. suggest that in an alternative embodiments, the motor vehicle could be any type of motor vehicle such as truck, bus, motorcycle, boat, snowmobiles, etc. Moreover, the security system could be utilized to control and grant access to a secure area such as a building, room, vault, cabinet or grant access to a secure database or any type of secure system (col. 3 line 63 to col. 4 lines 5) and Desai discloses the vehicle control teaches code to the key/fob combination. A series

of steps to move the key/fob combination into a learn mode is utilized, and then the code is then taught from the vehicle scanning receiver to the key/fob combination.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include key information retaining device (37) (i.e. key/fob combination) is a wireless operation device wirelessly connected to an information device (22) (i.e. control located in the vehicle) and includes a key information input module (48) (i.e. key pad) inputting the key information in contact with said key information issuing device (22), and said output module includes (i.e. transmitter of the control 22) a contact module outputting the key information in contact with said key information input module of Desai in the information issuing device of Bonder et al. in view of Cregger et al. and Weiss et al. with the motivation for doing so would allow the retaining device to communicate wirelessly with the issuing device as an alternative way of communicating through physical contact.

Referring to claim 31, Bonder et al. in view of Cregger et al., Weiss et al. and Desai disclose a readable-by-computer recording medium recorded with a program executed by a computer to manage key information issued to a key information retaining device, to the extent as claimed with respect to claim 30 above, Desai discloses the device further comprising: wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a medium input module (48) (i.e. key pad) inputting information from a recording medium, and said output module (i.e. transmitter of the vehicle control)

includes a recording medium write module writing the information to said recording medium, and issues the key information through said recording medium (col. 1 lines 48-57, col. 2 line 45 to col. 12 and col. 3 line 53 to col. 4 line 14; see Abstract and Figure 1). It is inherent for the key/fob and vehicle control with recording medium within in order to store the codes.

Referring to claim 32, Bonder et al. in view of Cregger et al., Weiss et al. and Desai disclose a readable-by-computer recording medium recorded with a program executed by a computer to manage key information issued to a key information retaining device, to the extent as claimed with respect to claim 30 above, Weiss et al. disclose the device further comprising: wherein said key information retaining device is a wireless operation device wirelessly connected to an information device and includes a near communication module incapable of performing communications beyond a predetermined distance, and said output module includes a near communication module incapable of performing the communications with said key information retaining device beyond a predetermined distance, and issues the key information through said near communication module (col. 3 lines 21-28 and col. 4 lines 1-10). (i.e. The near communication module of retaining device is incapable of communicating with the output module of the issuing device when is out-of-ranged).

Referring to claim 14,28,42,43,44,45,46,47 and 48, Bonder et al. in view of Cregger et al., Weiss et al. and Desai disclose a key information issuing device and

method according to claims 2,3,4,16,17,18,30,31 and 32, Weiss et al. disclose wherein said key information retaining device is an electronic key that unlocks a predetermined area (col. 1 lines 64-67). Weiss disclose a base station 10 is an access control system of an automobile or of a building by using the control element 20 to unlock within the accessing range.

Conclusion

Any inquiry concerning this communication or earlier communications form the examiner should be directed to Scott Au whose telephone number is (571) 272-3063. The examiner can normally be reached on Mon-Fri, 8:30AM – 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached at (571) 272-3068. The fax phone numbers for the organization where this application or proceeding is assigned are (571)-272-1817.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)-305-3900.

Scott Au

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600